PATENT ABSTRACTS OF JAPAN

(11)Publication number : **11-250193**
(43)Date of publication of application : **17.09.1999**

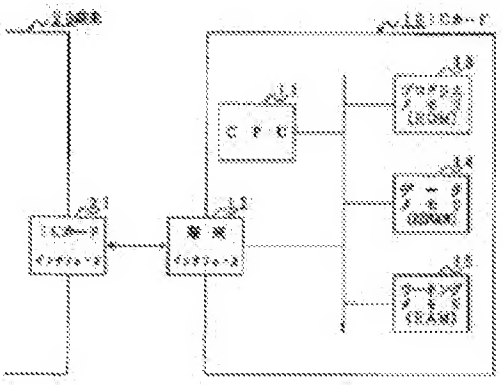
(51)Int.Cl. G06K 17/00
G06F 19/00
G07G 1/12

(21)Application number : **10-052133**
(22)Date of filing : **04.03.1998**

(71)Applicant : **OKI ELECTRIC IND CO LTD**
(72)Inventor : **KAMIMURA AKITOSHI**

(54) IC CARD AND ITS TRANSACTION PROCESSING METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To prevent the illegal use of an IC card and the illegal drawing of electronic money by setting a flag without fail before unlocking, releasing the flag after setting locking and setting locking in a case when the flag is previously set.
SOLUTION: The IC card 10 compares a password sent from a customer and a password previously registered in a data memory 14 and when the passwords are coincident with each other, the flag setting means of CPU 11 sets the flag 1 in the memory 14 by setting or clearing. Continually, the IC card 10 unlocks the locking by the unlocking means of CPU 11. Then, after unlocking, the IC card 10 executes prescribed processing by the processing means of CPU 11. Continually, after setting locking by the locking setting means of CPU 11, the IC card 10 releases the flag 1 by clearing or setting by the flag releasing means of CPU 11.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平11－250193

(43)公開日　平成11年(1999)９月17日

(51)Int.Cl.⁶	識別記号	ＦＩ	
Ｇ０６Ｋ　17/00		Ｃ０６Ｋ　17/00	Ｂ
			Ｌ
			Ｓ
Ｇ０６Ｆ　19/00		Ｃ０７Ｇ　1/12	３２１Ｐ
Ｇ０７Ｇ　1/12	３２１	Ｃ０６Ｆ　15/30	３５０

審査請求　未請求　請求項の数４　ＯＬ　（全７頁）

(21)出願番号　特願平10－52133

(22)出願日　平成10年(1998)３月４日

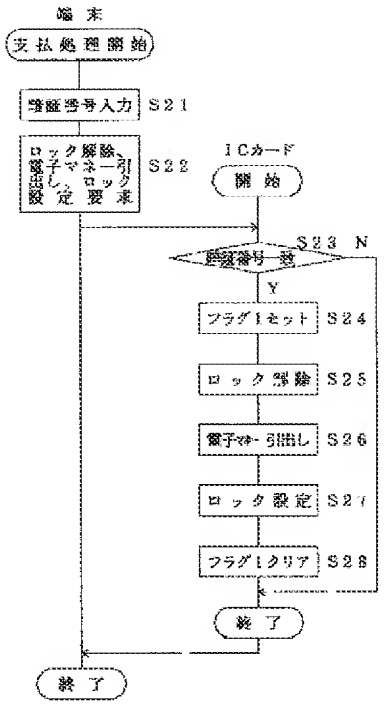
(71)出願人　000000295
沖電気工業株式会社
東京都港区虎ノ門１丁目７番12号

(72)発明者　上村　明利
東京都港区虎ノ門１丁目７番12号　沖電気工業株式会社内

(74)代理人　弁理士　川合　誠　（外１名）

(54)【発明の名称】　ＩＣカード及びその取引処理方法

(57)【要約】
【課題】ＩＣカードが不正に使用されることがなく、電子マネーが不正に引き出されることがないようにする。
【解決手段】端末からコマンドが送られたときに、内部に形成されたフラグを設定するフラグ設定手段と、フラグが設定された状態でロックを解除するロック解除手段と、ロックが解除された状態で所定の処理を行う処理手段と、処理が終了した後にロックを設定する第１のロック設定手段と、ロックが設定された後に前記フラグを解除するフラグ解除手段と、あらかじめフラグが設定されている場合に、ロックを設定する第２のロック設定手段とを有する。ロックを解除する前に、フラグが必ず設定され、ロックが設定された後にフラグが解除されるとともに、あらかじめフラグが設定されている場合に、ロックが設定される。



【特許請求の範囲】
【請求項１】　（ａ）端末からコマンドが送られたときに、内部に形成されたフラグを設定するフラグ設定手段と、（ｂ）前記フラグが設定された状態でロックを解除するロック解除手段と、（ｃ）前記ロックが解除された状態で所定の処理を行う処理手段と、（ｄ）前記処理が終了した後にロックを設定する第１のロック設定手段と、（ｅ）前記ロックが設定された後に前記フラグを解除するフラグ解除手段と、（ｆ）あらかじめフラグが設定されている場合に、ロックを設定する第２のロック設定手段とを有することを特徴とするＩＣカード。
【請求項２】　前記端末からの一つのコマンドに基づいて、前記ロック解除手段によるロックの解除、前記処理手段による所定の処理、及び前記第１のロック設定手段によるロックの設定が、一連の動作で排他的に行われる請求項１に記載のＩＣカード。
【請求項３】　前記処理手段は、あらかじめ設定された動作可能条件が満たされたときに前記処理を行う請求項１に記載のＩＣカード。
【請求項４】　（ａ）端末からＩＣカードにコマンドが送られたときに、ＩＣカードの内部に形成されたフラグを設定し、（ｂ）フラグが設定された状態でＩＣカードのロックを解除し、（ｃ）ロックが解除された状態で所定の処理を行い、（ｄ）処理が終了した後にＩＣカードのロックを設定し、（ｅ）該ロックが設定された後に前記フラグを解除するとともに、（ｆ）あらかじめ前記フラグが設定されている場合に、ＩＣカードにロックを設定することを特徴とするＩＣカードの取引処理方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、ＩＣカード及びその取引処理方法に関するものである。
【０００２】
【従来の技術】従来、電子マネーが充填（てん）されたＩＣカードは、商店等においてプリペイド方式又はポストペイド方式で使用されるようになっている。その場合、例えば、商店に設置された電子マネー用の端末の挿入・引出口に顧客又は店員がＩＣカードを差し込み、店員が前記端末を操作して支払額を入力すると、端末の表示部に支払額が表示されるようになっている。
【０００３】そして、店員が顧客に対して支払額の確認を求め、顧客が例えば、「ＹＥＳ」キーを押すと、端末とＩＣカードとの間において取引処理としての支払処理が開始され、支払額に相当する分の電子マネーがＩＣカードから引き出され、端末に入金される。続いて、前記表示部に支払処理が終了したことが表示されると、顧客又は店員はＩＣカードを端末の挿入・引出口から引き抜く。
【０００４】次に、前記ＩＣカードの支払処理について説明する。図２は従来のＩＣカードの支払処理方法を示すフローチャートである。まず、端末がＩＣカードにコマンドを送り、ＩＣカードのロック状態を問い合わせると、該ＩＣカードはロック状態を端末に応答する。このとき、端末は前記ＩＣカードからの応答に基づいて、ＩＣカードにおいてロックが設定されているかどうかを判断する。
【０００５】ところで、ＩＣカードにおいてロックが設定されている場合、電子マネーを引き出すことはできない。そこで、前記端末は、ロックが設定されている旨を表示部に表示し、顧客にロックを解除するための暗証番号を入力するよう促す。これに対して顧客が暗証番号を入力すると、端末は、ＩＣカードに暗証番号を送り、ロックを解除するよう要求する。
【０００６】続いて、ＩＣカードは、送られた暗証番号と内蔵するデータメモリにあらかじめ登録された暗証番号とを比較し、両暗証番号が一致すると、ロックを解除する。次に、端末は、ＩＣカードに引出額を送り、ＩＣカード内の電子マネーの引出しを要求する。そして、ＩＣカードは要求された電子マネーを引き出し、端末に入金する。このようにして、ＩＣカードから電子マネーが引き出されると、端末はＩＣカードにロックを設定するよう要求し、該ＩＣカードは端末からの要求に従ってロックを設定する。
【０００７】なお、ＩＣカードにおいてロックが設定されていない場合、端末は、ＩＣカードに引出額を送り、ＩＣカード内の電子マネーの引出しを要求する。そして、ＩＣカードは要求された電子マネーを引き出し、端末に入金する。次に、フローチャートについて説明する。
ステップＳ１　端末はＩＣカードのロック状態を問い合わせる。
ステップＳ２　ＩＣカードはロック状態を端末に応答する。
ステップＳ３　端末はＩＣカードにおいてロックが設定されているかどうかを判断する。ロックが設定されている場合はステップＳ４に、ロックが設定されていない場合はステップＳ８に進む。
ステップＳ４　暗証番号を入力する。
ステップＳ５　端末はＩＣカードにロックを解除するよう要求する。
ステップＳ６　ＩＣカードは、送られた暗証番号とデータメモリにあらかじめ登録された暗証番号とが一致するかどうかを判断する。暗証番号が一致した場合はステップＳ７に進み、一致しない場合は処理を終了する。
ステップＳ７　ＩＣカードはロックを解除する。
ステップＳ８　端末はＩＣカード内の電子マネーの引出しを要求する。
ステップＳ９　ＩＣカードは要求された電子マネーを引き出す。
ステップＳ１０　端末はＩＣカードにロックを設定する

よう要求する。
ステップＳ１１　ＩＣカードはロックを設定する。
【０００８】
【発明が解決しようとする課題】しかしながら、前記従来のＩＣカードにおいては、支払処理中にロックが解除された状態でＩＣカードが奪取された場合等にＩＣカードが不正に使用されると、電子マネーが不正に引き出されてしまう。本発明は、前記従来のＩＣカードの問題点を解決して、ＩＣカードが不正に使用されることがなく、電子マネーが不正に引き出されることがないＩＣカード及びその取引処理方法を提供することを目的とする。
【０００９】
【課題を解決するための手段】そのために、本発明のＩＣカードにおいては、端末からコマンドが送られたときに、内部に形成されたフラグを設定するフラグ設定手段と、前記フラグが設定された状態でロックを解除するロック解除手段と、前記ロックが解除された状態で所定の処理を行う処理手段と、前記処理が終了した後にロックを設定する第１のロック設定手段と、前記ロックが設定された後に前記フラグを解除するフラグ解除手段と、あらかじめフラグが設定されている場合に、ロックを設定する第２のロック設定手段とを有する。
【００１０】本発明のＩＣカードの取引処理方法においては、端末からＩＣカードにコマンドが送られたときに、ＩＣカードの内部に形成されたフラグを設定し、フラグが設定された状態でＩＣカードのロックを解除し、ロックが解除された状態で所定の処理を行い、処理が終了した後にＩＣカードのロックを設定し、該ロックが設定された後に前記フラグを解除する。
【００１１】そして、あらかじめ前記フラグが設定されている場合に、ＩＣカードにロックを設定する。
【００１２】
【発明の実施の形態】以下、本発明の実施の形態について図面を参照しながら詳細に説明する。図３は本発明の第１の実施の形態におけるＩＣカードの取引処理装置を示すブロック図である。図において、１０はＩＣカード、１１は該ＩＣカード１０の制御を行うＣＰＵ、１２は端末２０とのインタフェースを行う端末インタフェース、１３は制御プログラムを格納するプログラムメモリ（ＲＯＭ）、１４はデータが格納されるデータ不揮発性のデータメモリ（Ｅ２ＰＲＯＭ）、１５は前記ＩＣカード１０を動作させるためのワーキングメモリ（ＲＡＭ）、２１は前記ＩＣカード１０とのインタフェースを行うＩＣカードインタフェースである。なお、ＩＣカード１０及び端末２０によって取引処理装置が構成される。
【００１３】次に、前記ＩＣカード１０の取引処理としての支払処理について説明する。図１は本発明の第１の実施の形態におけるＩＣカードの支払処理方法を示すフローチャートである。まず、端末２０（図３）は、所定の表示を図示されない表示部に行い、顧客にロックを解除するための暗証番号を入力するよう促す。これに対して顧客が暗証番号を入力すると、端末２０は、ＩＣカード１０に暗証番号を送り、所定の一つのコマンドによって、ロックを解除するよう要求するとともに、ＩＣカード１０に引出額を送り、ＩＣカード１０内の電子マネーの引出し、及びロックの設定を要求する。
【００１４】続いて、ＩＣカード１０は、送られた暗証番号と前記データメモリ１４にあらかじめ登録された暗証番号とを比較し、両暗証番号が一致すると、ＣＰＵ１１の図示されないフラグ設定手段により、データメモリ１４内のフラグ１をセット又はクリアすることによって設定する。なお、本実施の形態においては、前記フラグ設定手段はフラグ１をセットする。続いて、前記ＩＣカード１０は、ＣＰＵ１１の図示されないロック解除手段によってロックを解除する。
【００１５】なお、両暗証番号が一致しない場合、ＩＣカード１０は前記各要求を拒否して支払処理を終了する。そして、ＩＣカード１０は、ロックを解除した後、ＣＰＵ１１の図示されない処理手段によって所定の処理を行う。なお、本実施の形態において、前記処理手段は、要求された電子マネーを引き出す。続いて、ＩＣカード１０は、ＣＰＵ１１の図示されない第１のロック設定手段によってロックを設定した後、ＣＰＵ１１の図示されないフラグ解除手段により、前記フラグ１をクリア又はセットすることによって解除する。なお、本実施の形態において、前記フラグ解除手段は、前記フラグ１をクリアする。
【００１６】次に、フローチャートについて説明する。
ステップＳ２１　暗証番号を入力する。
ステップＳ２２　端末２０は、ＩＣカード１０に暗証番号を送り、ロックの解除、電子マネーの引出し、及びロックの設定を要求する。
ステップＳ２３　ＩＣカード１０は、送られた暗証番号とデータメモリ１４にあらかじめ登録された暗証番号とが一致するかどうかを判断する。暗証番号が一致した場合はステップＳ２４に進み、一致しない場合は処理を終了する。
ステップＳ２４　フラグ１をセットする。
ステップＳ２５　ＩＣカード１０はロックを解除する。
ステップＳ２６　ＩＣカード１０は要求された電子マネーを引き出す。
ステップＳ２７　ＩＣカード１０はロックを設定する。
ステップＳ２８　フラグ１をクリアする。
【００１７】次に、ＩＣカード１０の初期化動作について説明する。図４は本発明の第１の実施の形態におけるＩＣカードの初期化動作を示すフローチャートである。まず、ＩＣカード１０（図３）は、データメモリ１４内のフラグ１をチェックし、フラグ１がセットされている

かどうかを判断する。そして、ＩＣカード１０は、前記フラグ１がクリアされている場合は、そのまま初期化動作を継続し、フラグ１がセットされている場合は、ＣＰＵ１１の図示されない第２のロック設定手段によってロックを設定した後、前記フラグ１をクリアし、そのまま初期化動作を継続する。

【００１８】次に、フローチャートについて説明する。

ステップＳ３１　フラグ１がセットされているかどうかを判断する。フラグ１がセットされている場合はステップＳ３２に、フラグ１がクリアされている場合はステップＳ３４に進む。

ステップＳ３２　ロックを設定する。

ステップＳ３３　フラグ１をクリアする。

ステップＳ３４　初期化動作を継続する。

【００１９】このように、本実施の形態においては、一つのコマンドがＩＣカード１０に送られるだけで、ＩＣカード１０は、ロックの解除、電子マネーの引出し、及びロックの設定から成る一連の動作を排他的に行うようになっているので、その間にＩＣカード１０に他のコマンドを送るのが困難になる。したがって、ロックが解除された状態でＩＣカード１０が不正に使用されることがなくなり、電子マネーが不正に引き出されることがない。

【００２０】また、ＩＣカード１０において、ロックを解除する前にフラグ１が必ずセットされ、ロックが設定された後にフラグ１がクリアされるとともに、初期化動作時において、ＩＣカード１０は、フラグ１をチェックし、フラグ１がセットされている場合、ロックを設定するようになっているので、支払処理中にロックが解除された状態でＩＣカード１０が奪取された場合、ＩＣカードを不正に使用しようとしても、フラグ１がセットされているので、初期化動作時においてＩＣカード１０が自らロックを設定することになる。したがって、ＩＣカード１０が不正に使用されることがなく、電子マネーが不正に引き出されることがない。

【００２１】なお、本実施の形態においては、一つのコマンドに基づいて、ロックの解除、電子マネーの引出し、及びロックの設定から成る一連の動作が排他的に行われるようになっているが、ロックの解除、電子マネーの引出し、及びロックの設定の各動作を別々のコマンドに基づいて行うこともできる。また、ＩＣカード１０は、初期化動作時にフラグ１をチェックし、該フラグ１がセットされている場合にロックを設定するようになっているが、端末２０からコマンドが送られたときに、コマンドを実行する前に前記フラグ１をチェックし、該フラグ１がセットされている場合にロックを設定することもできる。

【００２２】次に、本発明の第２の実施の形態について説明する。なお、第１の実施の形態と同じ構造を有するものについては、同じ符号を付与することによってその説明を省略する。図５は本発明の第２の実施の形態におけるＩＣカードの支払処理方法を示す第１のフローチャート、図６は本発明の第２の実施の形態におけるＩＣカードの支払処理方法を示す第２のフローチャートである。

【００２３】まず、端末２０（図３）は、所定の表示を図示されない表示部に行い、顧客にロックを解除するための暗証番号を入力するよう促す。これに対して顧客が暗証番号を入力すると、端末２０は、ＩＣカード１０に暗証番号を送り、所定のコマンドによって、ロックを解除するよう要求する。このとき、端末２０は、例えば、引出回数の最大値を１回に、引出金額の最大値を今回の引出額に設定してＩＣカード１０に送る。なお、本実施の形態においては、前記引出回数及び引出金額の各最大値によって動作可能条件が構成される。

【００２４】次に、ＩＣカード１０は、送られた暗証番号と前記データメモリ１４にあらかじめ登録された暗証番号とを比較し、両暗証番号が一致すると、ＣＰＵ１１の図示されないフラグ設定手段により、データメモリ１４内のフラグ２をセット又はクリアすることによって設定するとともに、端末２０から送られた引出回数及び引出金額の各最大値をデータメモリ１４に設定し、続いて、ＣＰＵ１１の図示されないロック解除手段によってロックを解除する。なお、本実施の形態においては、前記フラグ設定手段はフラグ２をセットする。

【００２５】また、両暗証番号が一致しない場合、ＩＣカード１０はロックを解除する旨の要求を拒否して支払処理を終了する。次に、端末２０は、ＩＣカード１０に引出額を送り、ＩＣカード１０内の電子マネーの引出しを要求する。これに対して、ＩＣカード１０は、フラグ２をチェックし、フラグ２がセットされている場合は、前記引出回数及び引出金額の各最大値をチェックして前記動作可能条件が満たされているかどうかを判断する。そして、前記動作可能条件が満たされている場合、すなわち、引出回数の最大値が０より大きく、引出金額が最大値以下である場合、引出回数及び引出金額の各最大値を更新し、引出回数の最大値を１だけ減算し、引出金額の最大値を今回の引出金額分だけ減算した後、ＣＰＵ１１の図示されない処理手段によって所定の処理を行う。なお、本実施の形態において、前記処理手段は、要求された電子マネーを引き出す。

【００２６】そして、前記フラグ２がクリアされている場合は、要求された電子マネーを引き出す。さらに、前記動作可能条件が満たされていない場合、すなわち、引出回数が０であり、引出金額が最大値より大きい場合は、引出エラーを応答する。そして、ＩＣカード１０から正常に電子マネーを引き出すことができると、端末２０は、ＩＣカード１０にロックを設定するよう要求する。続いて、ＩＣカード１０は、ＣＰＵ１１の図示されない第１のロック設定手段によってロックを設定した

後、ＣＰＵ１１の図示されないフラグ解除手段により、前記フラグ２をクリア又はセットすることによって解除する。なお、本実施の形態において、前記フラグ解除手段は、前記フラグ２をクリアする。

【００２７】次に、フローチャートについて説明する。

ステップＳ４１　暗証番号を入力する。

ステップＳ４２　端末２０はＩＣカード１０にロックを解除するよう要求する。

ステップＳ４３　ＩＣカード１０は、送られた暗証番号とデータメモリ１４にあらかじめ登録された暗証番号とが一致するかどうかを判断する。暗証番号が一致した場合はステップＳ４４に進み、一致しない場合は処理を終了する。

ステップＳ４４　フラグ２をセットし、引出回数及び引出金額の最大値を設定する。

ステップＳ４５　ＩＣカード１０はロックを解除する。

ステップＳ４６　端末２０はＩＣカード１０に電子マネーを引き出すよう要求する。

ステップＳ４７　ＩＣカード１０はフラグ２をチェックし、フラグ２がセットされているかどうかを判断する。フラグ２がセットされている場合はステップＳ４８に、フラグ２がセットされていない場合はステップＳ５０に進む。

ステップＳ４８　ＩＣカード１０は引出回数の最大値が０より大きく、引出金額が最大値以下であるかどうかを判断する。引出回数の最大値が０より大きく、引出金額が最大値以下である場合はステップＳ４９に、そうでない場合はステップＳ５１に進む。

ステップＳ４９　ＩＣカード１０は引出回数及び引出金額の最大値を更新し、引出回数の最大値を１だけ減算し、引出金額の最大値を今回の引出金額分だけ減算する。

ステップＳ５０　ＩＣカード１０は要求された電子マネーを引き出す。

ステップＳ５１　引出エラーを応答する。

ステップＳ５２　端末２０はＩＣカード１０にロックを設定するよう要求する。

ステップＳ５３　ＩＣカード１０はロックを設定する。

ステップＳ５４　フラグ２をクリアする。

【００２８】このように、本実施の形態においては、ＩＣカード１０において、ロックを解除する前に引出回数及び引出金額の最大値が設定されるとともに、電子マネーの引出しに伴って最大値が更新される。したがって、支払処理中にロックが解除された状態でＩＣカード１０が奪取された場合、ＩＣカードを不正に使用しようとしても、引出回数が０になるか、引出金額が最大値より大きくなると、電子マネーの引出しの要求が拒否されるので、ＩＣカード１０が不正に使用されることがなく、電子マネーが不正に引き出されることがない。

【００２９】なお、ＩＣカード１０は、ロックの解除が要求されると、引出回数の最大値を１回に、引出金額の最大値を今回の引出額に設定するようになっているが、端末２０において別のコマンドを発生させ、該コマンドによって任意の引出回数の最大値及び引出金額の最大値の原本をＩＣカード１０に送ることもできる。その場合、ＩＣカード１０は、前記最大値の原本をデータメモリ１４に格納し、ロックを解除するときに、データメモリ１４に格納された最大値の原本をチェック用の領域にコピーし、コピーされた最大値の原本を利用することもできる。

【００３０】前記各実施の形態においては、電子マネーが充填されたＩＣカードについて説明しているが、他のＩＣカードに適用することもできる。なお、本発明は前記実施の形態に限定されるものではなく、本発明の趣旨に基づいて種々変形させることが可能であり、それらを本発明の範囲から排除するものではない。

【００３１】

【発明の効果】以上詳細に説明したように、本発明によれば、ＩＣカードにおいては、端末からコマンドが送られたときに、内部に形成されたフラグを設定するフラグ設定手段と、前記フラグが設定された状態でロックを解除するロック解除手段と、前記ロックが解除された状態で所定の処理を行う処理手段と、前記処理が終了した後にロックを設定する第１のロック設定手段と、前記ロックが設定された後に前記フラグを解除するフラグ解除手段と、あらかじめフラグが設定されている場合に、ロックを設定する第２のロック設定手段とを有する。

【００３２】この場合、ＩＣカードにおいて、ロックを解除する前にフラグが必ず設定され、ロックが設定された後にフラグが解除されるとともに、あらかじめフラグが設定されている場合に、ロックが設定される。したがって、処理中にロックが解除された状態でＩＣカードが奪取された場合、ＩＣカードを不正に使用しようとしても、フラグがセットされているので、ＩＣカードが自らロックを設定することになる。したがって、ＩＣカードが不正に使用されることがなく、電子マネーが不正に引き出されることがない。

【図面の簡単な説明】

【図１】本発明の第１の実施の形態におけるＩＣカードの支払処理方法を示すフローチャートである。

【図２】従来のＩＣカードの取引処理方法を示すフローチャートである。

【図３】本発明の第１の実施の形態におけるＩＣカードの支払処理装置を示すブロック図である。

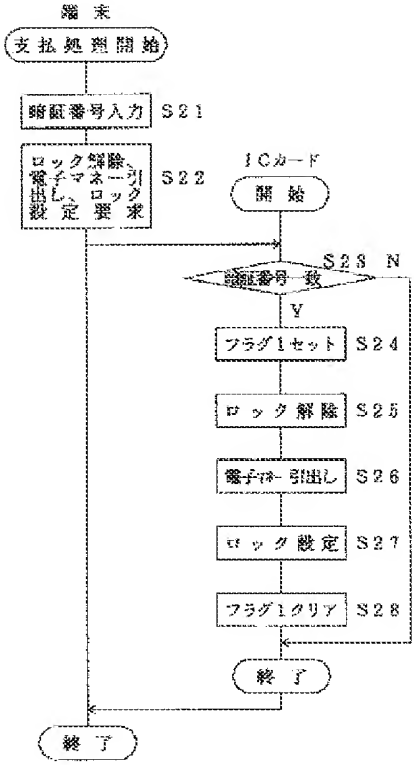
【図４】本発明の第１の実施の形態におけるＩＣカードの初期化動作を示すフローチャートである。

【図５】本発明の第２の実施の形態におけるＩＣカードの支払処理方法を示す第１のフローチャートである。

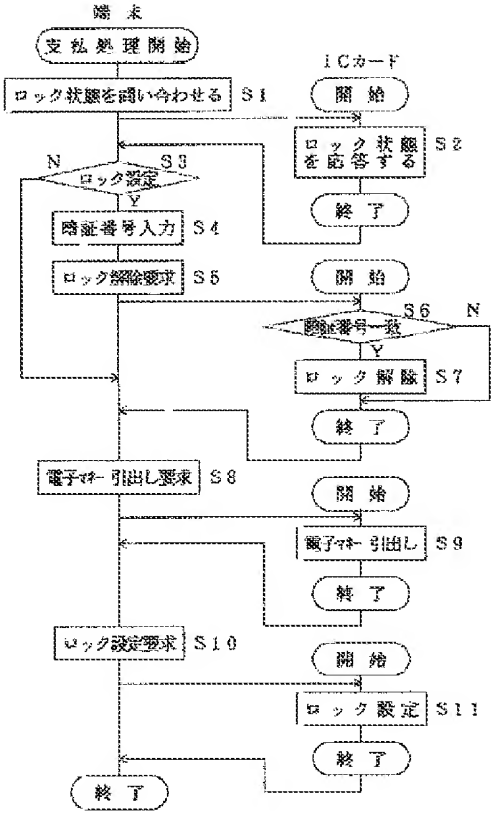
【図６】本発明の第２の実施の形態におけるＩＣカードの支払処理方法を示す第２のフローチャートである。

【符号の説明】
10　ICカード
11　CPU
20　端末

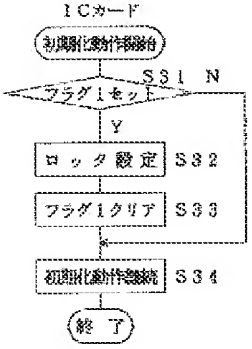
【図1】



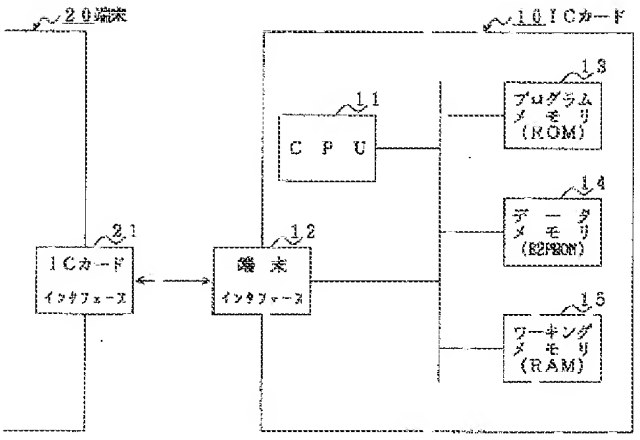
【図2】



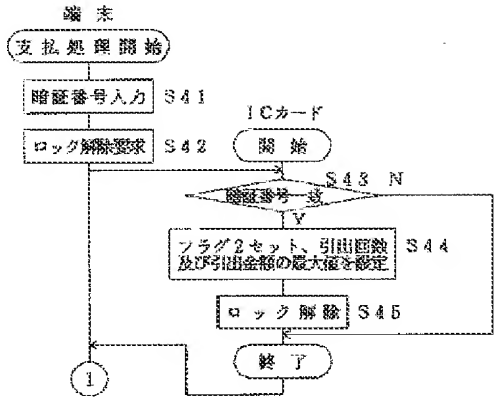
【図4】



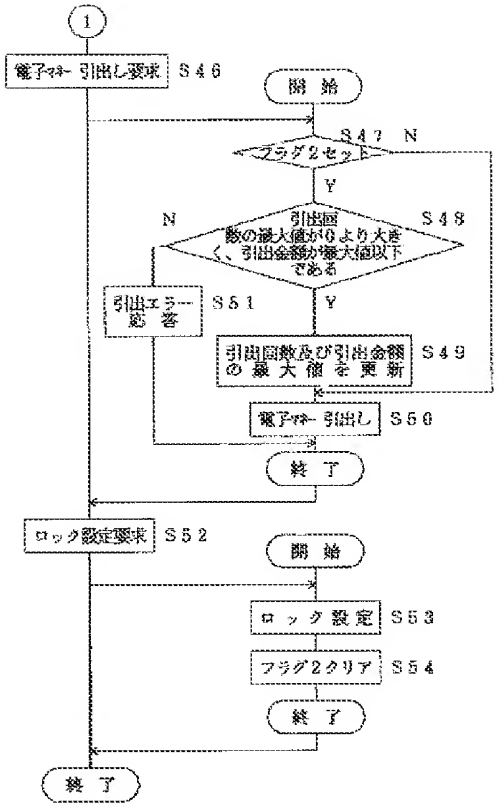
【図3】



【図5】



【図６】


①
電子ﾏﾈｰ引出し要求
S46
開始
S47
N
フラグ2セット
Y
N
引出回数の最大値が0より大きく、引出金額が最大値以下である
S48
Y
引出エラー処理
S51
引出回数及び引出金額の最大値を更新
S49
電子ﾏﾈｰ引出し
S50
終了
ロック設定要求
S52
開始
ロック設定
S53
フラグ2クリア
S54
終了
終了